IN THE CLAIMS

1. (Canceled)

2. (Currently amended) A method as in claim ~~1~~38, wherein the stored object information is descriptive at least in part of a number and location of macros within the object.

3. (Currently amended) A method as in claim ~~1~~38, wherein the stored object information is descriptive at least in part of a number and location of archived objects within the object.

4. (Currently amended) A method as in claim ~~1~~38, wherein the stored object information is descriptive at least in part of features of the object that serve as inputs to a neural network-based virus detection system, and wherein the step of programmatically examining the object comprises a step of operating the neural network-based virus detection system using the features as inputs.

5. (Currently amended) A method as in claim ~~1~~38, wherein the stored object information is descriptive at least in part of whether at least one macro is present within the object.

6. (Currently amended) A method as in claim ~~1~~38, wherein the stored object information is descriptive at least in part of whether at least one archived object is present within the object.

7. (Currently amended) A method as in claim ~~1~~38, wherein the stored object information is descriptive at least in part of whether the object can possibly be infected with a virus according to predetermined criteria, and wherein the step of programmatically examining is executed only if the stored object information

2

indicates that the object may possibly be infected according to the predetermined criteria as compared to criteria that are currently in effect.

8. (Currently amended) A method as in claim 138, wherein if it is indicated that a current state of the object is not described by the stored object information, the step of programmatically examining comprises an initial step of processing the object to ascertain the current state of the object, and storing information in the object-state database that is descriptive of the current state of the object.

9. (Currently amended) A method as in claim 138, wherein the stored object information comprises, for an object that contains in archived or combined form at least one other object, information descriptive of whether the at least one contained object is of a type that should be examined for computer viruses, and wherein the step of programmatically examining avoids re-determining and re-scanning the contained at least one object if the stored object information indicates that the at least one contained object is not required to be scanned.

10. (Currently amended) A method as in claim 138, wherein the stored object information comprises, for an object that contains in archived or combined form at least one other object, information descriptive of at least one of a location, extent, or encoding-method of the at least one contained object, and wherein the step of programmatically examining is responsive to the stored object information for reducing an amount of processing time required to extract the at least one contained object in order to examine the at least one contained object.

11. (Currently amended) A method as in claim 138, wherein the stored object information comprises information descriptive of a location of an entry-point of the object, and wherein the step of programmatically examining uses the stored object information to determine the entry-point of the object, if the object-state database indicates that the object has not changed since the entry-point information was stored.

3

12. (Currently amended) A method as in claim ~~13~~8, wherein the stored object information comprises information descriptive of a structure of the object, and wherein the step of programmatically examining uses the stored object information to determine the structure of the object, if the object-state database indicates that the object has not changed since the structure information was stored.

13. (Currently amended) A method as in claim ~~13~~8, wherein the stored object information comprises information descriptive of at least one of a number, size, name, extent, or other attribute of macros or other units of active content in the object, and wherein the step of programmatically examining uses the stored object information to determine at least one of the number, size, name, extent, or other attribute of macros or other units of active content in the object, if the object-state database indicates that the object has not changed since the information was stored.

14. (Currently amended) A method as in claim ~~13~~8, wherein the step of programmatically examining includes a program-emulation step for executing the current object in a virtual environment, for collecting data resulting from the execution in the virtual environment, and for storing at least some of the results produced by the program-emulation step in the object-state database, and wherein the step of programmatically examining uses the stored results rather than re-executing the program-emulation step, if the object-state database indicates that the object has not changed since the results were stored.

15. (Canceled)

16. (Currently amended) A virus detection component as in claim ~~15~~39, wherein the stored object information is descriptive at least in part of a number and location of macros within the object.

4

17. (Currently amended) A virus detection component as in claim ~~15~~39, wherein the stored object information is descriptive at least in part of a number and location of archived objects within the object.

18. (Currently amended) A virus detection component as in claim ~~15~~39, wherein the stored object information is descriptive at least in part of features of the object that serve as inputs to a neural network-based virus detection system, and wherein said neural network-based virus detection system uses the features as inputs.

19. (Currently amended) A virus detection component as in claim ~~15~~39, wherein the stored object information is descriptive at least in part of whether at least one macro is present within the object.

20. (Currently amended) A virus detection component as in claim ~~15~~39, wherein the stored object information is descriptive at least in part of whether at least one archived object is present within the object.

21. (Currently amended) A virus detection component as in claim ~~15~~39, wherein the stored object information is descriptive at least in part of whether the object can possibly be infected with a virus according to predetermined criteria, and wherein said object examination unit programmatically examines said object only if the stored object information indicates that the object may possibly be infected according to the predetermined criteria as compared to criteria that are currently in effect.

22. (Currently amended) A virus detection component as in claim ~~15~~39, wherein if said determination indicates that a current state of the object is not described by the information stored in said database, said object examination unit first processes the object to ascertain the current state of the object, and stores

information in said <u>object-state</u> database that is descriptive of the current state of the object.

23. (Currently amended) A virus detection component as in claim ~~15~~39, wherein the stored <u>object</u> information comprises, for an object that contains in archived or combined form at least one other object, information descriptive of whether the at least one contained object is of a type that should be examined for computer viruses, and wherein said object examination unit inhibits re-determining and re-scanning the contained at least one object if the stored <u>object</u> information indicates that the at least one contained object is not required to be scanned.

24. (Currently amended) A virus detection component as in claim ~~15~~39, wherein the stored <u>object</u> information comprises, for an object that contains in archived or combined form at least one other object, information descriptive of at least one of a location, extent, or encoding-method of the at least one contained object, and wherein said object examination unit is responsive to the stored <u>object</u> information for reducing an amount of processing time required to extract the at least one contained object in order to examine the at least one contained object.

25. (Currently amended) A virus detection component as in claim ~~15~~39, wherein the stored <u>object</u> information comprises information descriptive of a location of an entry-point of the object, and wherein said object examination unit is responsive to the stored <u>object</u> information to determine the entry-point of the object, if the <u>object-state</u> database indicates that the object has not changed since the entry-point information was stored.

26. (Currently amended) A virus detection component as in claim ~~15~~39, wherein the stored <u>object</u> information comprises information descriptive of a structure of the object, and wherein said object examination unit is responsive to the stored <u>object</u> information for determining the structure of the object, if the

object-state database indicates that the object has not changed since the structure information was stored.

27. (Currently amended) A virus detection component as in claim ~~15~~39, wherein the stored object information comprises information descriptive of at least one of a number, size, name, extent, or other attribute of macros or other units of active content in the object, and wherein said object examination unit is responsive to the stored object information for determining at least one of the number, size, name, extent, or other attribute of macros or other units of active content in the object, if the object-state database indicates that the object has not changed since the information was stored.

28. (Currently amended) A virus detection component as in claim ~~15~~39, and further comprising a program-emulation unit for executing the current object in a virtual environment, for collecting data resulting from the execution in the virtual environment, and for storing at least some of the results produced by the program-emulation unit in said database, and wherein said object examination unit is responsive to the stored results for using said stored results, and for inhibiting the operation of said program emulation unit, if the object-state database indicates that the object has not changed since the results were stored.

29. (Canceled)

30. (Currently amended) A computer program as in claim ~~29~~40, wherein said computer readable medium further stores a list comprised of information that is descriptive of at least one of known viruses and of known classes of viruses, said list being used by said object examination code segment when programmatically examining the object for the presence of a computer virus.

31. (Currently amended) A computer program as in claim ~~29~~40, wherein said computer readable medium further stores a neural network-based virus detection

code segment, wherein said object-state database further stores information descriptive of features of the object that serve as inputs to said neural network-based virus detection code segment, and wherein said neural network-based virus detection code segment uses the features as inputs.

32. A computer program as in claim 2940, wherein said computer readable medium further stores a program-emulation code segment for executing objects in a virtual environment, for collecting data resulting from the execution in the virtual environment, and for storing at least some of the results in said database, and wherein said object examination unit code segment is responsive to the stored results for using said stored results, and for inhibiting the operation of said program emulation unit code segment, if said object-state database indicates that the object has not changed since the results were stored.

33. (Canceled)

34. (Currently amended) A computer program as in claim 3341, wherein the stored object information is descriptive at least in part of a number and location of macros within the object.

35. (Currently amended) A computer program as in claim 3341, wherein the stored object information is descriptive at least in part of a number and location of archived objects within the object.

36. (Currently amended) A computer program as in claim 3341, wherein the computer program implements or has access to a neural network-based virus detection system, wherein the stored object information is descriptive at least in part of features of the object that serve as inputs to the neural network-based virus detection system, and wherein the step of programmatically examining the object comprises a step of operating the neural network-based virus detection system using the features as inputs.

37. (Currently amended) A computer program as in claim ~~33~~41, wherein for an object that the <u>object-state</u> database indicates has a current state that is not described by the stored <u>object</u> information, the step of programmatically examining comprises an initial step of operating the stored program to process the object to ascertain the current state of the object, and storing information in the <u>object-state</u> database that is descriptive of the current state of the object.

38. (New) A virus detection method for use in a computer system, comprising steps of:

providing an object-state database comprised of stored object information that is descriptive of a state of at least one object that may potentially become infected by a computer virus and that reflects the state of said object as it existed at a point in the past;

providing a virus-detection database comprised of virus-detection information used in programmatically examining objects for the presence of various computer viruses;

for a current scan of said object that is indicated as having a current state that is described by the stored object information, determining whether or not said object appears to have changed since said point in the past; and

in the case that said object does not appear to have changed since said point in the past, but said virus-detection database does appear to have changed since said point in the past, programmatically examining said object for a presence of a computer virus while making use of the stored object information during the examination.

39. (New) A virus detection component for use in a computer system, comprising:

an object-state database comprised of stored object information that is descriptive of a state of at least one object that may potentially become infected by a computer virus and that reflects the state of said object as it existed at a point in the past;

a virus-detection database comprised of virus-detection information used in programmatically examining objects for the presence of various computer viruses; and

an object examination unit, which, for a current scan of said object that is indicated as having a current state that is described by the stored object information, determines whether or not said object appears to have changed since said point in the past; and which, in the case that said object does not appear to have changed since said point in the past, but said virus-detection database does appear to have changed since said point in the past, programmatically examines said object for a presence of a computer virus while making use of the stored object information during the examination.

40. (New) A computer program embodied on a computer-readable medium for providing a virus detection program subsystem, comprising:

a code segment that at least maintains an object-state database comprised of stored object information that is descriptive of a state of at least one object that may potentially become infected by a computer virus and that reflects the state of said object as it existed at a point in the past;

a virus detecting code segment that at least maintains a virus-detection database comprised of virus-detection information used in programmatically examining objects for the presence of various computer viruses; and

an examination code segment, which, for a current scan of said object that is indicated as having a current state that is described by the stored object information, determines whether or not said object appears to have changed since said point in the past; and which, in the case that said object does not appear to have changed since said point in the past, but said virus-detection database does appear to have changed since said point in the past, programmatically examines said object for a presence of a computer virus while making use of the stored object information during the examination.

41. (New) A computer program embodied on a computer-readable medium, the computer program being capable of executing a method for use in a computer system that comprises at least one object that may potentially become infected with a computer virus, the method executed by the computer program comprising steps of:

maintaining an object-state database comprised of stored object information that is descriptive of a state of at least one object that may potentially become infected by a computer virus and that reflects the state of said object as it existed at a point in the past;

maintaining a virus-detection database comprised of virus-detection information used in programmatically examining objects for the presence of various computer viruses;

for a current scan of said object that is indicated as having a current state that is described by the stored object information, determining whether or not said object appears to have changed since said point in the past; and

11

in the case that said object does not appear to have changed since said point in the past, but said virus-detection database does appear to have changed since said point in the past, programmatically examining said object for a presence of a computer virus while making use of the stored object information during the examination.